Safeguard Computer Security Evaluation Matrix (SCSEM)

Application Security Controls

Release IV

May 26, 2009

Internal
Revenue
Service

Tester:	*Insert Tester Name*
Date:	*Insert Date(s) Testing Occurred*
Location:	*Insert Location testing was conducted*
Agency POC(s):	*Insert each Agency interviewee(s) name, address, phone number and email address.*
Application Name:	*Insert the name of the application and a description of its function for FTI processing*
Application Vendor (COTS):	*Insert name of vendor if application is COTS*
Source Code Information (Custom-built):	*Insert application language used (C, C++, Java, PHP, ASP, etc)*

SCSEM Results Dashboard

Status	**# of Tests**	**Percent (%)**
Pass	0	#DIV/0!
Fail	0	#DIV/0!
Info	0	#DIV/0!
Not Applicable	0	#DIV/0!
Blank (Not Reviewed)	82	100.0%
Total Tests Performed	0	-
Total # Tests Available	82	-

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
1	AC-11	DISA Application Security Checklist V2 R1.1 3420	FISCAM AS 2.3.2	COTS/ Custom	The application provides the ability to manually log off of the application. The application automatically logs off the user's account (AS 2.3.2)	1. Test the application by logging in as a user and attempt to manually log out. If this option is not available, ask the Application Administrator to explain how this function is performed. 2. Examine system security settings or observe an idle user session to determine whether the application logs the user off after an elapsed period of idle time.	1. The application provides the ability for a user to manually initiate a log out and the log out feature is reasonably accessible to the user. *Note: Reasonable accessibility is defined as the user having a hyperlink or button which they can click to manually log off. It is also acceptable if the application automatically logs a user off after the closing of the application or web browser.* 2. Idle application sessions are logged off after 15 minutes of inactivity.			
2	AC-2	DISA Application Security Checklist V2 R1.1 6210	FISCAM AS 2.4.3	COTS/ Custom	The agency has implemented an account management process for the application. Access is limited to individuals with a valid business purpose (least privilege) (AS 2.4.3)	1. Interview the Application Administrator to verify documented operating procedures exist for user and system account creation, termination, and expiration. 2. Examine a list of users added to the application within the past month and select a sample to determine the proper account authorization is is in place. 3. Examine a list of recently departed personnel and verify that their accounts were removed or deactivated on all systems in a timely manner (e.g., less than two days).	1. The Application Administrator can demonstrate that documented operating procedures exist. 2. The sampled accounts have the proper authorization in place in accordance with agency policy. 3. The list of active accounts does not contain personnel who have recently departed the agency or no longer need access.			
3	AC-6	DISA Application Security Checklist V2 R1.1 3190		COTS/ Custom	Database connections from the application use non-administrative accounts.	*Note: This test case is only applicable to a database backend which stores FTI and accessed from a front-end interface such as a webpage.* 1. Interview the Application Administrator and determine the account used in the database connection string. 2. Examine the account used in the database connection string on the operating system to verify the type and privilege level of the account.	2. The application uses a non-administrative account to access the database.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
4	AC-3	DISA Application Security Checklist V2 R1.1 3240	FISCAM AS 3.8	COTS/ Custom	Determine if the application permits only authorized transactions. (AS 3.8)	1. Interview the Application Administrator and determine how the application authorizes transactions. Determine which of the following applies to the application: • A transaction authorization mechanism is built into the application code. If so, ask the application developer to locate the modules in the code that perform the authorization function. Review these to assess their adequacy. • Transaction authorization controlled through file permissions established by the operating system or views enforced by the database software. If the application leverages the access controls of the database or operating system software, identify cases in which permissions are granted to everyone, world, public or similar user, or group for which all users would be authorized. *Note: The actual code review need not occur on a production system so long as the code reviewed is equivalent to the production code.*	1. The application code or the access controls of supporting software provide appropriate controls preventing unauthorized users from performing transactions that require authorization. 2. For any resource that is granted to everyone, world, public or similar user, it is the stated intention that the resource be public such that everyone will be authorized access.			
5	AC-3	DISA Application Security Checklist V2 R1.1 3360	FISCAM AS 2.7	COTS/ Custom	Ensure identification and authentication information is protected by appropriate file permissions. Sensitive application resources (identification & authentication information) are adequately protected. (AS 2.7)	Interview the Application Administrator and determine how user credentials are stored. 1. Examine the permission configuration of the file, folder or database table where the credentials are stored. 2. If user credentials are stored in a databases table, determine the encryption used on that table. *Note: In many cases, local backups of the accounts database exist so these must be included in the scope of the review.*	1. Only administrators, and the application or OS process that access the information should have permissions to access identification and authentication information. 2. Database tables containing account credentials are encrypted.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
6	AC-3	DISA Application Security Checklist V2 R1.1 3450		Custom	Format strings are restricted to authorized personnel.	1. Examine the locations of all format strings used by the application. Ask the Application Administrator to demonstrate format strings used by the application are restricted to authorized users.	1. Modification of format strings is restricted to authorized personnel only.			*Note: Format string vulnerabilities occur when specially crafted format strings passed to a function allow flow control information to be viewed or modified. In a worst-case scenario, format string vulnerabilities can allow an attacker to execute code of their choice on the system, resulting in complete system compromise.*
7	AC-5	DISA Application Security Checklist V2 R1.1 3480	FISCAM AS 4.3.3	COTS/ Custom	The application enforces a separation of duties for sensitive administrator roles. User access to transactions or activities that have segregation of duties conflicts is appropriately controlled. There is an effective segregation of duties between the security administration function of the application and the user functions. (AS 4.3.3)	1. Interview the Application Administrator to identify the following: • Personnel that review and clear audit logs • Personnel that perform non-audit administration. 2. Interview the Application Administrator to identify the following: • Personnel that create, modify, and delete access control rules • Personnel that perform either data entry or application programming. 3. Interview the Application Administrator to identify the following: • Personnel that have access as a security administrator	1. Personnel who review and clear audit logs are separate from personnel that perform non-audit administration. 2. Personnel who create, modify, and delete access control rules are separate from personnel that perform data entry or application programming. 3. Personnel with security administration do not have access to input, process, or approve transactions; do not have access to more than application security administration functions and are prevented from accessing production data.			
8	AC-5	FISCAM AS 4.1 FISCAM AS 4.2		COTS/ Custom	Incompatible transactions and activities have been identified. Application controls prevent users from performing incompatible duties	1. Inquire if management has prepared a separation of duties matrix or uses commercially available software to monitor segregation of duties. 2. Determine through inquiry, observation, and inspection how the application segregates users from performing incompatible duties. 3. For a selected sample of users, inspect their access profiles to determine whether the access is appropriate and if any of the users have access to menus with conflicting duties.	1. Users are prevented by the application from executing incompatible transactions, as authorized by the business owners.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
9	AC-5	FISCAM AS 4.4		COTS/ Custom	User access to transactions or activities that have separation of duties conflicts is appropriately controlled.	1. Inspect user administration policy to determine whether owner approval is required to access transactions or activities in their area of responsibility. 2. Interview administrators to determine that access authorization requests are reviewed for separation of duties prior to granting access. Inspect a representative form, noting approval and consideration of segregation of duties. 3. Interview owners and inspect documentation to determine whether appropriate procedures are in place to identify and remove or modify access as appropriate to ensure segregation of duties.	1. Owners authorize users to have access to transactions or activities that cause segregation of duty conflicts only when it supports a business need. 2. Security administrators review application user access authorizations for segregation of duties conflicts and discuss any questionable authorizations with owners. 3. Owners periodically review access to identify unauthorized segregation of duties conflicts.			
10	AC-5	FISCAM AS 4.5		COTS/ Custom	Effective monitoring controls are in place to mitigate segregation of duties risks.	1. Inspect documentation of roles and users with conflict. Determine if management uses commercially available software to determine segregation of duties violations. If so, determine if appropriate follow up action is taken. Review evidence of monitoring of control effectiveness.	1. Process owners have identified the segregation of duty conflicts that can exist, and the roles and users with conflicts.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
11	AC-6	DISA Application Security Checklist V2 R1.1 3470	FISCAM AS 2.6	COTS/ Custom	The application does not permit non-privileged users the ability to perform any administrative tasks. User access to sensitive transactions or activities is appropriately controlled. (AS 2.6)	1. Log on as an unprivileged user. Examine the user interfaces (graphical, web, and command line) to determine if any administrative functions are available. Privileged functions include the following: • Create, modify and delete user accounts and groups • Grant, modify, and remove file or database permissions • Configure password and account lockout policy • Configure policy regarding the number and length of sessions • Change passwords or certificates of users other than oneself • Determine how the application will respond to error conditions • Determine auditable events and related parameters • Establish log sizes, fill thresholds, and fill behavior (i.e., what happens when the log is full)	1. Non-privileged users do not have the ability to perform the identified functions. *Note: Results should specify which of the functions are not restricted to privileged users.*			
12	AC-6	DISA Application Security Checklist V2 R1.1 3500		COTS/ Custom	Application accounts do not have excessive privileges. Access to the application is restricted to authorized users. (AS2.4) Access is limited to individuals with a valid business purpose (least privilege) (AS2.4.3) Master data are complete and valid.(BP 4.4)	1. Identify the account(s) that the application uses to run. These accounts include the application processes (defined by Control Panel Services (Windows) or ps –ef (UNIX). Also for an n-tier application, the account that connects from one service (such as a web server) to another (such as a database server). 2. Examine the user groups in which each account is a member. List the user rights assigned to these users and groups and evaluate whether any of them are unnecessary. For example, if the user did not execute the transaction or activity within the expected time frame, processes should be in place to evaluate the continued need for access, and modify access accordingly.	1. Rights assigned to the user(s) are necessary. • The account is not a member of the Administrators group (Windows) or has a User Identification (UID) of 0 (i.e., is equivalent to root in UNIX). • The account is not a member of the SYSAdmin fixed server role in SQL Server • The account does not have DDL (Data Definition Language) privileges, (create, drop, alter) or other system privileges. • There are no instances of unnecessary ownership or permissions.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
13	AC-7	DISA Application Security Checklist V2 R1.1 3390	FISCAM AS 2.3.2	COTS/ Custom	The application enforces user account lockout. The application locks the users account after a pre-determined number of attempts to log-on with an invalid password. The application may automatically reset the account after a specific time period (an hour to day) or may require an administrator to reset the account. (AS 2.3.2)	1. Test the application with a valid user account to verify if a user enters a password incorrectly more than three consecutive times. 2. Examine the application setting for account lockout if the setting exists.	1. The user account is locked after three consecutive incorrect attempts.			
14	AC-7	DISA Application Security Checklist V2 R1.1 3400		COTS/ Custom	Only an administrator can unlock locked accounts.	1. Interview the Application Administrator and verify that only the administrator can unlock locked user accounts.	1. Only administrators can unlock accounts that have been locked.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
15	AC-8	DISA Application Security Checklist V2 R1.1 3440		COTS/ Custom	The application displays an approved warning banner.	1. Logon to the application. Verify that the warning banner displayed is in compliance with IRS requirements. The user must accept the warning banner message before moving forward.	1. The warning banner should display the following or equivalent text: This system may contain Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to Criminal and Civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording and analysis of all data being communicated, transmitted, processed or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel. ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.			*Reviewer Note: This test may also be performed by the DES as part of the disclosure review. Coordinate with the DES for the collection of evidence for this control.*
16	AC-14	NIST SP 800-53A		COTS/ Custom	User actions that can be performed without identification and authentication are documented.	1. Examine the application to determine if there are any user actions that can be performed on the information system without identification or authentication.	1. If any actions are available without identification and authentication they are limited to general information that is publicly available. 2. For any other user actions that can be performed without identification and authenticaiton, the agency has identified and documented specific user actions that can be performed on the information system without identification or authentication			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
17	AU-9	DISA Application Security Checklist V2 R1.1 6140		COTS/ Custom	Audit trails cannot be read or modified by non-administrator users.	1. Interview the application administrator to determine the application audit log location. 2. Examine the permission settings of the log files. For a Windows system, the NTFS file permissions should be System – Full control, Administrators and Application Administrators - Read, and Auditors - Full Control. For UNIX systems, use the ls –la (or equivalent) command to check the permissions of the audit log files.	1. Log files have appropriate permissions assigned and permissions are not excessive.			
18	AU-2	DISA Application Security Checklist V2 R1.1 3640		COTS/ Custom	Transaction logs exist that record access and changes to the data.	1. Test the application by having the Application Administrator login as an unprivileged user and perform actions to demonstrate the application creates transaction logs for access and modifications to FTI. 2. Review the transaction log to verify the actions were written to the log.	1. The actions performed were written to the transaction log.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
19	AU-2	DISA Application Security Checklist V2 R1.1 3680	FISCAM AS 2.9	COTS/ Custom	The application adequately logs security-relevant events. Application Security violations are identified in a timely manner. (AS 2.9)	1. Examine audit logs and ensure the following events are captured in accordance with IRS Publication 1075: • All successful login and logoff attempts. • All unsuccessful login and authorization attempts. • All identification and authentication attempts. • All actions, connections and requests performed by privileged users. • All actions, connections and requests performed by privileged functions. • All changes to logical access control authorities (e.g., rights, permissions). • System changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services. • Creation, modification and deletion of objects (e.g. files, directories and user accounts) • Creation, modification and deletion of user accounts and group accounts • Creation, modification and deletion of user account and group account privileges. • System startup and shutdown functions. • Modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-e • Enabling or disabling of audit report genera • Command line changes, batch file changes • The audit trail shall be protected from unaut	1. The identified audit events are captured in the application logs. • All successful login and logoff attempts. • All unsuccessful login and authorization attempts. • All identification and authentication attempts. • All actions, connections and requests performed by privileged users. • All actions, connections and requests performed by privileged functions. • All changes to logical access control authorities (e.g., rights, permissions). • System changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services. • Creation, modification and deletion of objects (e.g. files, directories and user accounts) • Creation, modification and deletion of user accounts and group accounts • Creation, modification and deletion of user account and group account privileges. • System startup and shutdown functions. • Modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleti • Enabling or disabling of audit report genera • Command line changes, batch file changes • The audit trail shall be protected from unaut			
20	AU-3	NIST SP 800-53A		COTS/ Custom	The application produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.	1. Examine a sample audit log from the application to determine if the application audit records capture 1) sufficient information to establish what events occurred; 2) sufficient information to establish the sources of the events; 3) sufficient information to establish the outcomes of the events.	1. The application audit log captures the sufficient information to establish what events occurred, the sources of the events and the outcomes of the events, for example: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service or process responsible for initiating the system event.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
21	AU-4	DISA Application Security Checklist V2 R1.1 3650		COTS/ Custom	Notification is provided when audit logs are reaching near capacity.	1. Examine the application documentation and ask the Application Administrator what automated mechanism is in place to ensure the administrator is notified when the application logs are near capacity. 2. If the Application Administrator or the documentation indicates a mechanism is in place, examine the configuration of the mechanism to ensure the process is present and executing.	1. An automated mechanism is in place to warn the administrator. 2. The automated mechanism works as described.			
22	AU-5	DISA Application Security Checklist V2 R1.1 6090		COTS/ Custom	The system alerts in a low resource condition.	1. Examine the application configuration to determine if an automated, continuous on-line monitoring and audit trail creation capability is present with the capability to immediately alert personnel of any unusual or inappropriate activity, or in the event the audit process fails and logs are not being written.	1. The system's monitoring capability works as described.			
23	AU-6 AC-13	DISA Application Security Checklist V2 R1.1 6110	FISCAM AS 2.10	COTS/ Custom	Audit trails are periodically reviewed by security personnel. Exceptions and violations are properly analyzed and appropriate actions are taken (AS 2.10)	1. Interview Application Administrator and ask for the system documentation that states how often audit logs are reviewed. Also, determine when the last audit logs were reviewed. 2. Examine reports of that demonstrate monitoring of security violations, such as unauthorized user access.	1. The Application Administrator can provide system documentation identifying how often the auditing logs are reviewed. The auditing logs have been reviewed by security personnel within the time period identified in the system documentation.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
24	CM-2	DISA Application Security Checklist V2 R1.1 2020		COTS/ Custom	The Application Baseline Configuration is Documented	1. Examine the application configuration guide or equivalent document to determine if information such as the following is documented: • Versions of Compliers used • Build options when creating application/components • Versions of COTS Software Used as part of the application • For web applications, which browsers and what versions are supported All Known security assumptions, implications, system level protections, best practices, and required permissions are documented in the Application Configuration Guide. All Deployment configuration settings are documented in the Application Configuration Guide. Examples include: • Encryptions Settings • PKI Certificate Configuration Settings • Password Settings	1. The following information is documented in the application configuration guide: • Versions of Compliers used • Build options when creating application/components • Versions of COTS Software Used as part of the application • For web applications, which browsers and what versions are supported All Known security assumptions, implications, system level protections, best practices, and required permissions are documented in the Application Configuration Guide. All Deployment configuration settings are documented in the Application Configuration Guide. Examples include: • Encryptions Settings • PKI Certificate Configuration Settings • Password Settings			*Reviewer Note: This test may overlap with the CM control tests executed as part of the MOT SCSEM.*
25	CM-3	DISA Application Security Checklist V2 R1.1 4030	FISCAM AS 3.1	COTS/ Custom	A Software Configuration Management Plan Exists AS 3.1 Policies and procedures are designed to reasonably assure that changes to application functionality in production are authorized and appropriate, and unauthorized changes are detected and reported promptly (AS 3.1)	1. Examine the Software Configuration Management (SCM) Plan or equivalent document. The SCM plan should contain the following: • Description of the configuration control and change management process • Types of objects developed • Roles and responsibilities of the organization 2. Interview the application administrator to identify key transactions that provide user access to application change functionality. 3. Inspect transaction reports of changes made to the application. For sample of changes, inspect documentation of changes made, validity, reasons, authorization, and user authority.	1. The SCM plan contains a description of the configuration control and change management process, types of objects developed, and roles and responsibilities of the organization. 2. The transaction reports indicate changes to application functionality are authorized and appropriate.			*Reviewer Note: This test may overlap with the CM control tests executed as part of the MOT SCSEM.*

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
26	CM-3	DISA Application Security Checklist V2 R1.1 4040	FISCAM AS 3.4	COTS/ Custom	The Agency Uses a Configuration Control Board (CCB) to Govern the Application. Authorizations for changes are documented and maintained (AS 3.4)	1. Interview the Application Administrator to determine if a configuration control board exists and identify the primary members. Ask if there is CCB charter documentation, and examine the documentation. 2. Interview the application administrator to determine how often the configuration control board meets. Ask if there is CCB charter documentation. The CCB charter documentation should indicate how often the CCB meets. 3. Identify recent software modification and determine whether change request forms were used and if CCB approval is documented. *Note: If there is no charter documentation, ask when the last time the CCB met, and when was the last release of the application. CCB's do not have to physically meet and the CCB chair may authorize a release based on phone and/or email conversations*	1. The agency has implemented a CCB for the FTI system and CCB charter documentation is available. 2. The CCB charter documentation indicates how often the CCB meets. 3. Software modifications made are approved by the CCB.			*Reviewer Note: This test may overlap with the CM control tests executed as part of the MOT SCSEM.*
27	CM-4	DISA Application Security Checklist V2 R1.1 5040		COTS/ Custom	Application Changes and Upgrades are Assessed for Security Impact Changes are controlled as programs progress through testing to final approval. (AS 3.5)	1. Examine the CCB process documentation to ensure potential changes to the application are evaluated to determine impact. An informal group may be tasked with impact assessment of upcoming version changes.	1. The agency performs an impact analysis for the FTI system.			*Reviewer Note: This test may overlap with the CM control tests executed as part of the MOT SCSEM.*
28	CM-5	DISA Application Security Checklist V2 R1.1 4010	FISCAM AS 3.11	Custom	Access rights to the CM repository are periodically reviewed. Access and changes to programs and data are monitored (AS 3.11)	1. Interview the Application Administrator and verify how frequently the configuration management repository access permissions are reviewed. 2. Examine evidence of the most recent review of the CM repository access rights.	1. The configuration management repository access permissions are reviewed at least every three months. 2. The person reviewing the CM repository access should not have the authority to make changes.			*Reviewer Note: This test may overlap with the CM control tests executed as part of the MOT SCSEM.*

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
29	CM-5	DISA Application Security Checklist V2 R1.1 4010		Custom	Access restrictions for changes to the application are in place.	1. Examine the CM repository permissions to determine the rights granted to users.	1. A single user cannot request, test, verify, and move a single change request to production.			*Reviewer Note: This test may overlap with the CM control tests executed as part of the MOT SCSEM.*
30	CM-6	DISA Application Security Checklist V2 R1.1 2020	FISCAM AS 3.2	COTS/ Custom	Approved security configuration guidance is used to configure application security features.	1. Examine the agency security policy for security configuration of custom built applications.	1. The agency establishes and documents mandatory security configuration settings for custom built applications. 2. The application is compliant with the agency's security configuration policy.			*Reviewer Note: This test may overlap with the CM control tests executed as part of the MOT SCSEM.*
31	CM-6	DISA Application Security Checklist V2 R1.1 6020	FISCAM AS 3.2	COTS	COTS products are configured to agency security configuration policy. Current configuration information is maintained (AS3.2)	1. Examine the agency security policy for configuration of COTS applications.	1. The agency establishes and documents mandatory security configuration settings for COTS applications. 2. The COTS application is compliant with the agency's security configuration policy.			*Reviewer Note: This test may overlap with the CM control tests executed as part of the MOT SCSEM.*
32	CM-7	DISA Application Security Checklist V2 R1.1 3110 6030		COTS	Unneeded functionality is disabled.	1. Interview the Application Administrator to determine what functionality is installed and enabled by default for the application. 2. Examine the configuration of the server the application runs on. Determine what software is installed on the servers. Determine which services are needed for the application by examining the system documentation and interviewing the Application Administrator. For example, if two web servers (IIS and Apache) are installed and only one is being used.	1. The application does not install with functionality which is unnecessary and enabled by default. Any functions installed by default that are not required by the application are disabled. 2. Services or software which are not needed are not present on the server.			*Reviewer Note: This test may overlap with the CM control tests executed as part of the MOT SCSEM.*
33	IA-2	DISA Application Security Checklist V2 R1.1 3380	FISCAM AS 2.2	COTS/ Custom	The Application Does Not Contain Duplicate Accounts Application users are appropriately identified and authenticated (AS 2.2) Identification and authentication is unique to each user (AS 2.2)	1. Examine the list of application user accounts. 2. Test the application by attempting to create a new user account with the same name as an existing user account.	1. All application user accounts are unique, there are no duplicate user accounts. 2. The new user account creation fails. The application provides a mechanism to ensure duplicate user account names are not created, e.g., using operating systems functions to manage user accounts.			*Note: The results should specify the duplicates by name, unless they are too numerous to document, in which case a numerical count of the IDs is more appropriate.*

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
34	IA-2	DISA Application Security Checklist V2 R1.1 3460	FISCAM AS 2.3	COTS/ Custom	The Application Does Not Allow Blank Passwords Security policies and procedures appropriately address ID and password management (AS 2.3)	1. Test the application by attempting to create a new user account with a blank password. 2. Test the application by attempting to logon to the application with an existing user account, but leaving the password field blank.	1. The new user account creation fails, a password is required to create an account. 2. The logon attempt fails, a password is required for identification and authentication to the application.			
35	IA-5 AC-12	DISA Application Security Checklist V2 R1.1 3410	FISCAM AS 2.3.4	COTS/ Custom	The Number of Application Logon Sessions is Limited Multiple log-ons are controlled and monitored (AS 2.3.4)	1. Interview the application administrator to identify application modules that involve user or process sessions (e.g., a user may initiate a session with a web server, which in turn maintains sessions with a backend database server). 2. Examine the application configuration to determine if application provides system definable parameters for the following: -The total number of user sessions open for the entire application. -The total number of concurrent sessions that can be opened by a single user. -The total amount of idle time before the user session is forced to terminate. 3. If configuration parameters cannot be viewed, manually test conduct manual tests for the three items above. 4. If there is a business need for allowing multiple concurrent sessions opened by a single user, interview the application administrator to determine how it is monitored to ensure that segregation of duties conflicts are not created.	1. The application provides a capability to limit the total number of users sessions that can be opened in the entire application at the same time. 2. The application limits the number of concurrent sessions that can be opened by a single user to one. 3. The application automatically terminates a user session after 15 minutes of idle time. 4. A logical separation of duties is in place; if this is not feasible, an administrative policy is in place to enforce separation of duties.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
36	IA-5	DISA Application Security Checklist V2 R1.1 3350	FISCAM AS 2.7	Custom	Sensitive Information Is Not Embedded In Application Code Sensitive application resources are adequately protected (AS 2.7)	1. Examine application source code (including global.asa, if present), configuration files, scripts, HTML file, and any ascidia files to locate any instances in which a password, certificate, or sensitive data is included in the code.	1. No passwords, certificates or sensitive data are embedded in the code. *Note: The results should note specifically where the credentials or data were located and what resources they enabled.*			Tool
37	IA-5	DISA Application Security Checklist V2 R1.1 6240	FISCAM AS 2.6.4	COTS/ Custom	User Accounts Are Disabled After 90 Days of Inactivity Inactive accounts and accounts for terminated individuals are disable or removed in a timely manner (AS 2.6.4)	1. Examine the list of application user accounts to identify all users that have not authenticated in the past 90 days. *Note: If the user accounts used in the application are only operating system or database accounts this check is Not Applicable.*	1. All accounts found that have not authenticated in the past 90 days are disabled.			
38	IA-5	DISA Application Security Checklist V2 R1.1 6250	FISCAM AS 2.3	COTS/ Custom	Built-In Accounts Are Removed Security policies and procedures appropriately address ID and password management (AS 2.3)	1. Examine the list of application user accounts to identify any default built-in accounts (e.g., accounts with vendor names such as Oracle or Tivoli). *Note: Built-in accounts are those that are added as part of the installation of the application software. These accounts exist for many common commercial off-the-shelf (COTS) or open source components of enterprise applications (e.g., OS, web browser or database software).*	1. All default built-in accounts have been removed from the application or disabled if they cannot be removed.			
39	IA-5	DISA Application Security Checklist V2 R1.1 6260	FISCAM AS 2.3	COTS/ Custom	Default Passwords Have Been Changed Security policies and procedures appropriately address ID and password management (AS 2.3)	1. Test the application by attempting to authenticate with the published default password for any existing built-in account noted in Test ID #38, if such a default password exists. *Note: This test will require the reviewer to research ahead of time built-in accounts and default passwords for the application used by the agency, which will be identified during the PSE.*	1. All application default passwords have been changed from their default values.			
40	IA-5	FISCAM AS 2.3		COTS/ Custom	The application enforces agency password policy.	1. Test the application by creating a new user account and attempt to create a password that does not conform to agency password policy.	1. The attempt to create the password fails because it does not conform to agency password policy.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
41	IA-6	DISA Application Security Checklist V2 R1.1 3310	FISCAM AS 2.3	COTS/ Custom	Clear Text Passwords are Not Displayed During Login Security policies and procedures appropriately address ID and password management (AS 2.3)	1. Test the application by attempting to authenticate. Observe the screen output during password entry.	1. The password is not displayed in clear text, it is blotted by characters, i.e., asterisks.			
42	IA-7	NIST SP 800-53A		COTS/ Custom	The application employs authentication methods that meet the requirements of FIPS 140-2 for authentication to a cryptographic module.	1. Examine the application or documentation describing the current configuration settings to determine if the authentication mechanism uses a FIPS 140-2 compliant encryption module.	1. The application's authentication mechanism uses a FIPS 140-2 compliant encryption module.			
43	SA-11	DISA Application Security Checklist V2 R1.1 5010		COTS/ Custom	The Application is Periodically Tested for Security Flaws	1. Interview the application administrator to determine if the application is periodically tested for security flaws. 2. Examine test results from recent application security testing.	1. The application is tested for security flaws on a periodic basis using automated vulnerability scanning methods, or manual control testing, or a combination of both. 2. Test results are documented, and security flaws found during the test are entered into a tracking system and monitored for mitigation.			
44	SA-11	DISA Application Security Checklist V2 R1.1 5080		Custom	Code Reviews are Performed Prior to Application Release	1. Examine results from the code review performed on the application prior to its release in production. *Note: This test does not apply to COTS applications.*	1. A code review was performed on the application prior to release into production using automated or manual code analysis techniques, or a combination of both. 2. Security flaws found during the code review are entered into a defect tracking system and monitored for mitigation.			
45	SA-8	DISA Application Security Checklist V2 R1.1 2060 3130		Custom	Secure Design Principles and Coding Standards are Used for Application Development	1. Interview the application administrator to determine if a documented set of security design principles and coding standards exists. 2. Examine the documented set of security design principles.	1. A documented set of security principles and coding standards exists and is followed by agency application developers. 2. The documented set of security design principles are consistent with NIST SP 800-27.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
46	SA-8	DISA Application Security Checklist V2 R1.1 3010		COTS/ Custom	Application Design Documentation Exists	1. Examine the application's design documentation.	1. The design documentation covers many aspects of the application design but also documents the minimal security requirements for FTI, external interfaces, roles, access for the roles defined, and any unique security requirements.			
47	SC-13	DISA Application Security Checklist V2 R1.1 3150		COTS/ Custom	The Application Uses FIPS 140-2 Validated Encryption	1. Interview the application administrator to Identify all application features that require cryptography. 2. Verify the application is using FIPS 140-2 validated cryptographic modules. *The National Institute of Standards and Technology's (NIST) FIPS 140-2 Vendor List is located at: http://csrc.nist.gov/cryptval/.*	1. All cryptographic functions used by the application use FIPS 140-2 validated modules.			
48	SC-13	DISA Application Security Checklist V2 R1.1 3340		COTS/ Custom	Stored Passwords are Encrypted	1. Examine the configuration of the application software to determine if encryption settings have been activated to encrypt user IDs and passwords that are stored by the application.	1. User IDs and passwords stored by the application are encrypted using a FIPS 140-2 validated encryption mechanism.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
49	SC-18	DISA Application Security Checklist V2 R1.1 3700 3720 3740		COTS/ Custom	Mobile Code is Used Securely	1. Interview application administrator and examine application documentation to determine if mobile code is used. Verify the source of the mobile code and if it is signed. *Note: If the application does not contain mobile code this test is not applicable.* *Mobile code includes the following:* *1) ActiveX controls* *2) Mobile code scripts executing in Windows Scripting Host (WSH) (e.g., JavaScript,* *VBScript downloaded via URL file reference or email attachments)* *3) HTML Applications (e.g., hta files) downloaded as mobile code* *4) Scrap objects (e.g., .shs and .shb files)* *5) Windows and Microsoft Disk Operating System (MS-DOS) batch scripts (.cmd and .bat)* *6) UNIX Shell Scripts* *7) Binary executables (e.g., .exe files) downloaded as mobile code.* *8) Java applets and other Java mobile code* *9) VBA* *10) LotusScript (e.g., Lotus Notes scripts)* *11) PerfectScript (e.g., Corel Office macros)* *12) Postscript* *13) Mobile code executing in .NET Common Language Runtime*	1. Mobile code is obtained from a trusted source, and is designated as trusted. The mobile code is digitally signed and the digital signature is properly validated by the client runtime environment prior to the execution. 2. Unsigned mobile code operating in a constrained environment has no access to local operating system resources and does not attempt to establish network connections to servers other than the application server. *Note: The following mobile code types can be used without restriction:* *1) JavaScript and VBScript when used in a browser* *2) Portable Document Format (PDF)* *3) Flash animations executing in the Shockwave Flash Plugin*			
50	SC-2	DISA Application Security Checklist V2 R1.1 3060		COTS/ Custom	The Application Code is Separated from the FTI	1. Interview the application administrator or examine the application documentation to determine the location of the application code. 2. Examine the directory where the application code is located, to include both custom source code and COTS executable files.	1. The application code is not located in the same directory as the FTI.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
51	SC-2	DISA Application Security Checklist V2 R1.1 3070	FISCAM AS 2.1	COTS/ Custom	User Interface is Separated from Data Storage Application boundaries are adequately protected (AS 2.1)	1. Interview the application administrator to determine if a logical separation between user interfaces and data exist within the application. 2. Examine locations of the components of the application such as web server, database server, and application server. 3. Review security plans for proper identification of application boundaries	1. Separation is accomplished through the use of different computers, different CPUs, different instances of the operating system, different network addresses, or combinations of these methods, or other methods. *Note: A separate physical machine is not required but is recommended.*			
52	SC-2	FISCAM AS 3.6		COTS/ Custom	Access to program libraries is restricted.	1. Examine libraries in use. 2. Verify that source code exists for a selection of production code modules by (1) comparing compile dates (2) recompiling source modules and (3) comparing the resulting module size to production load module size. 3. Test access to program libraries by examining security system parameters.	1. Separate libraries are maintained for program development and maintenance, testing, and production programs. 2. Source code is maintained in a separate library. 3. Access to all programs, including production code, source, code and extra program copies are protected by access control software and operating system features.			
53	SC-4	DISA Application Security Checklist V2 R1.1 3100 3230		COTS/ Custom	The Application Removes Temporary Objects and Clears Memory Blocks	1. Test the application by logging into the application and performing selected actions. Then exit the application, and search for files recently created. For a Windows system: Use Windows Explorer to search for all files (*.*) created today, and then examine the times to narrow the scope of the files to examine. For a UNIX system: Enter: # touch -t 200301211020 /tmp/testdatefile 2. Ask the application administrator to demonstrate how the application clears and releases memory blocks.	1. Files are not found; temporary files are deleted automatically upon application exit. 2. The application clears objects prior to releasing memory.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
54	SC-4	DISA Application Security Checklist V2 R1.1 3430		COTS/ Custom	The Application Removes Authentication Credentials on Client Computers After a Session Terminates	1. Test the application by logging into the application and performing several standard operations, noting if the application ever prompts the user to accept a cookie. 2. Log out, close the browser and check the cookies directory on the server (e.g., /Windows/cookies, /Windows/profiles/xyz/cookies, and the /Documents and Settings/xyz/cookies directories (where xyz is replaced by the Windows user profile name)). 3. If a cookie has been placed in either of these directories, open it (using Notepad or another text editor) and search for identification or authentication data that remains after to check for sensitive application data	1. No authentication credentials are found in the cookie file (e.g., user name, ID, password, or key properties) 2. If the application is a web-based application, Internet Explorer (IE) is set to warn the user before accepting a cookie.			
55	SC-5	DISA Application Security Checklist V2 R1.1 6040		COTS/ Custom	Administrators Receive System Security Updates Automatically	1. Interview the application administrator to demonstrate deployment personnel (i.e., system administrators, database administrators, application administrators) are registered to receive notifications for updates to all the application components including and custom developed software.	1. Deployment personnel are registered to receive updates to all components of the application for example, Web Server, Application Servers, Database Servers. Also if update notifications are provided to any custom developed software, deployment personnel should also register for these updates.			
56	SC-7	DISA Application Security Checklist V2 R1.1 2100		COTS/ Custom	The Network Architecture Protects the Application From External Exposure	1. Examine network diagram that depicts the location of the application server(s).	1. All externally accessible application servers are in a demilitarized zone (DMZ).			
57	SC-8	DISA Application Security Checklist V2 R1.1 3090		COTS/ Custom	The Application Protects Against Session Hijacking	1. Interview the application administrator to login and demonstrate the application supports detection and/or prevention of communication session hijacking, i.e., integrity checks (e.g., hash algorithms, checksums).	1. The application uses integrity checks (e.g., hash algorithms, checksums) to detect errors in data streams of the application data transmitted over the network.			
58	SC-8	DISA Application Security Checklist V2 R1.1 3260		COTS/ Custom	The Application Supports Integrity Checking Mechanisms	1. Interview the application administrator to demonstrate the application supports mechanisms assuring the integrity of transmitted information, both incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs).	1. The application supports integrity checking mechanisms for file transmissions.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
59	SC-8 SC-9	DISA Application Security Checklist V2 R1.1 3250		COTS/ Custom	FTI is Encrypted In Transit Over WAN	1. Interview the application administrator to determine if FTI is transmitted over a wide area network (WAN) outside of the agency's local area network (LAN).	1. If FTI is transmitted over a wide area network, it is encrypted with FIPS 140-2 validated encryption.			
60	SC-9	DISA Application Security Checklist V2 R1.1 3330		COTS/ Custom	Passwords are Encrypted Prior to Transmission	1. Interview the application administrator to demonstrate passwords are encrypted before they are transmitted during authentication with FIPS 140-2 validated encryption.	1. The application encrypts passwords before they are transmitted during authentication with FIPS 140-2 validated encryption.			
61	SC-23	NIST SP 800-53A		COTS/ Custom	The application provides mechanisms to protect the authenticity of communications sessions.	1. Examine application design documentation, or other relevant documents; reviewing for session-level protection mechanisms and their configuration settings to be employed in the information system. *Note: The focus of this control is the information system protecting communications at the session, versus packet, level by implementing session level protection where needed.*	1. The application provides a capability to protect the authenticity of for session layer communication protocols used by the application.			
62	SI-9	FISCAM BP 1.4		COTS/ Custom	Input data are approved	1. Inspect documented procedures for approval of input data. 2. Inspect a selection of source documents (a sample is not required, but auditor could elect to choose one) and input files and determine whether the source data were approved for input.	1. Documented approval procedures exist to validate input data before entering the system. 2. Approval procedures are followed for data input.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
63	SI-10	DISA Application Security Checklist V2 R1.1 3510	FISCAM BP 1.5	COTS/ Custom	The Application Validates Input Input data are validated and edited to provide reasonable assurance that erroneous data are detected before processing (BP 1.5)	1. Examine the most recent application test plan to determine if testing was performed for invalid input, including the presence of scripting tags within text fields, query string manipulation, SQL command, and invalid data types and sizes. 2. Test the application by logging on to the application and entering invalid data in input fields. If there are various user types defined within the system, this test should be repeated for all user types. 3. Identify key data input screens and observe edits and validations that occur on data prior to acceptance.	1. The test plan and results indicate that input validation was tested. 2. The invalid data is rejected by the application. The application performs validation checks for known good data and rejects data that does not meet the criteria.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
64	SI-10	DISA Application Security Checklist V2 R1.1 3530		COTS/ Custom	The Application Sets the Character Set	1. Interview the application administrator to demonstrate if the application sets the character set to reduce the possibility of receiving unexpected input that uses other character set encodings. 2. Test the application by viewing web pages to determine the character set. The character set could be found in the following locations: Perl After the last header look for print "Content-Type: text/html; charset=utf-8\n\n"; PHP. Look for the header() function before any content is generated header('Content-type: text/html; charset=utf-8'); Java Servlets. Look for the setContentType method on the ServletResponse object Objectname.setContentType ("text/html;charset=utf-8"); JSP. Look for a page directives <%@ page contentType="text/html; charset=UTF-8" %> ASP Look for Response.charset	1. The application sets the character set to reduce the possibility of receiving unexpected input that uses other character set encodings by the web application.			
65	SI-10	DISA Application Security Checklist V2 R1.1 3540		COTS/ Custom	The Application is Protected Against SQL Injection	1. Examine the most recent code review results from the entire application. This can be provided as results from an automated code review tool, or a report that details vulnerabilities identified from a code review.	1. The code review results indicate the application is not vulnerable to SQL injection.			
66	SI-10	DISA Application Security Checklist V2 R1.1 3550		COTS/ Custom	The Application is Protected Against Integer Overflow	1. Examine the most recent code review results from the entire application. This can be provided as results from an automated code review tool, or a report that details vulnerabilities identified from a code review.	1. The code review results indicate the application does not contain integer overflow vulnerabilities.			http://www.owasp.org/index.php/Integer_overflow

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
67	SI-10	DISA Application Security Checklist V2 R1.1 3560		COTS/ Custom	The Application Does Not Contain Format String Vulnerabilities	1. Examine the most recent code review results from the entire application. This can be provided as results from an automated code review tool, or a report that details vulnerabilities identified from a code review.	1. The code review results indicate the application does not contain format string vulnerabilities.			http://www.owasp.org/index.php/Format_string_problem
68	SI-10	DISA Application Security Checklist V2 R1.1 3570		COTS/ Custom	The Application is Protected Against Command Injection	1. Examine the most recent code review results from the entire application. This can be provided as results from an automated code review tool, or a report that details vulnerabilities identified from a code review.	1. The code review results indicate the application is not vulnerable to command injection.			http://www.owasp.org/index.php/Command_Injection
69	SI-10	DISA Application Security Checklist V2 R1.1 3580		COTS/ Custom	The Application is Protected Against Cross Site Scripting	1. Examine the most recent code review results from the entire application. This can be provided as results from an automated code review tool, or a report that details vulnerabilities identified from a code review.	1. The code review results indicate the application is not vulnerable to cross site scripting.			http://www.owasp.org/index.php/Cross_Site_Scripting
70	SI-10	DISA Application Security Checklist V2 R1.1 3590		COTS/ Custom	The Application is Protected Against Buffer Overflows	1. Examine the most recent code review results from the entire application. This can be provided as results from an automated code review tool, or a report that details vulnerabilities identified from a code review. 2. Test the application by logging on the application and entering data larger than the application is expecting: • Very large number including large precision decimal numbers in numeric data fields. • Both negative and positive numbers should be included in numeric data fields. • Large amounts of data (at least 1024K) into the text fields. • If the application is a web-based application that utilizes query strings, testing should include passing at least 500 characters of data into the query string parameter.	1. The code review results indicate the application is not vulnerable to buffer overflows. 2. The application gives an error that indicates the error condition is being checked.			http://www.owasp.org/index.php/Buffer_Overflow

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
71	SI-10	DISA Application Security Checklist V2 R1.1 3600		COTS/ Custom	The Application is Protected Against Canonical Representation Attacks	1. Examine the most recent code review results from the entire application. This can be provided as results from an automated code review tool, or a report that details vulnerabilities identified from a code review.	1. The code review results indicate the application is not vulnerable to canonical representation attacks.			http://www.owasp.org/index.php/Canonicalization,_locale_and_Unicode
72	SI-10	DISA Application Security Checklist V2 R1.1 3630		COTS/ Custom	The Application is Protected Against Race Conditions	1. Examine the most recent code review results from the entire application. This can be provided as results from an automated code review tool.	1. The code review results indicate the application is not vulnerable to race conditions.			https://www.owasp.org/index.php/Reviewing_Code_for_Race_Conditions
73	SI-11	DISA Application Security Checklist V2 R1.1 3120		COTS/ Custom	The Application Handles Errors Properly	*Use the error messages generated from Test ID 63 as input into this check. Ensure that the application provides error-handling processes. The application code should not rely on internal system generated error handling.* 1. Inspect the verbiage of the messages to ensure that the application does not provide information that can be used by an attacker.	1. Error messages do not include variable names, variable types, SQL strings, or source code. Errors do not contain field names from the screen and a description of what should be in the field.			
74	SI-11	FISCAM BP 1.7		COTS/ Custom	Error handling procedures during data origination and entry reasonably assure that errors and irregularities are detected, reported, and corrected.	1. Inspect documented procedures related to data entry error handling procedures. 2. Inquire of management to determine which key management reports are used to monitor input errors. 3. Select a sample of input error reports and inspect to note evidence of management review. As applicable, inspect subsequent data input reports to note where data was corrected and resubmitted for processing.	1. Procedures are established to reasonably assure that all inputs into the application have been accepted for processing and accounted for; and any missing or unaccounted for source documents or input files have been identified and investigated. The procedures specifically require the exceptions to be resolved within a specific time period.			
75	SI 11	FISCAM BP 1.8		COTS/ Custom	Errors are investigated and resubmitted for processing promptly and accurately.	1. Inspect a recent error report and note whether suspense items are being corrected in a timely manner. 2. If there are any long-standing items on the suspense report, note management's reasons for not correcting them in a timely manner.	1. Data input errors are identified in suspense or error reports and resolved or resubmitted in a timely manner (within the period specified in the procedures			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
76	SI-11	DISA Application Security Checklist V2 R1.1 APP3140		COTS/ Custom	The Application Fails in a Secure State	1. Examine previous application test plans to determine if testing was performed to verify security remains in place when an application failure occurs (e.g., the application, web server or database service is stopped).	1. Test results indicate that the application fails closed when a failure occurs, e.g., when the application, web server or database service is stopped: -Application data is still protected -The database requires authentication before returning data -The application source files cannot be accessed because the application is not operating -Data is not available because the application is not operational			
77	SI-11	DISA Application Security Checklist V2 R1.1 5060		COTS/ Custom	The Application is Secure During Startup and Shutdown	1. Examine previous application test plans to ensure system initialization, shutdown, and aborts keep the system in a secure state.	1. Tests are conducted at least annually to ensure system initialization, shutdown, and aborts keep the system in a secure state.			
78	SI-11	DISA Application Security Checklist V2 R1.1 5100		COTS/ Custom	Fuzz Testing is Performed Prior to Application Releases	1. Examine previous application test plans to verify fuzz testing procedures are included and to determine if fuzz testing was performed prior to application releases. *Note: Fuzz testing injects automatically semi-random data into a program/stack and detect bugs. It is important that all critical applications, most notably those facing the Internet or those that consume and parse files be fuzzed.*	1. The test plan includes fuzz testing procedures (using an automated fuzzer) and fuzz testing is performed prior to all application releases. Fuzz test procedures include testing the User Interface (testing all the buttons sequences / text inputs), the command-line options, the import/export capabilities, and for a web application, the URLs, forms, user-generated content, RPC requests, etc.			http://www.owasp.org/index.php/Fuzzing
79	SI-12	FISCAM BP 3.5		COTS/ Custom	Access to output/reports and output files is based on business need and is limited to authorized users.	1. Select output/reports and output files from the audit area and inspect application access (if the output can be accessed on-line or other electronic form) or inspect distribution to determine whether the user has appropriate level of security clearance and is authorized to access	1. Access to reports is restricted to those users with a legitimate business need for the information. 2. Users should have appropriate authorization for accessing reports, including the appropriate level of security clearance, where applicable.			

Test ID	NIST ID (800-53)	Source	Source #2	Platform	Test Objective	Test Steps	Expected Results	Actual Results	Pass / Fail	Comments / Supporting Evidence
80	SI-2	DISA Application Security Checklist V2 R1.1 2130	FISCAM AS 3.13	COTS/ Custom	Application Maintenance is in Place Applications are updated in a timely manner to protect against known vulnerabilities (AS 3.13)	1. Interview the application administrator to determine if maintenance is readily available for the application and if the application is under vendor support to address security flaws identified in the application. 2. 1. Determine whether vendor supplied updates have been implemented. *Note: The vendor maintenance aspect of this test does not apply to custom developed applications supported by agency personnel. This test requires the tester to research the current vendor supplied patch level.*	1. The application is currently under support (either through vendor support for COTS product, or in-house agency maintenance team), and maintenance is available to address any security flaws discovered in the application. 2. The application is current with vendor supplied updates.			
81	SI-2	DISA Application Security Checklist V2 R1.1 3050		COTS/ Custom	Unused Code and Libraries are Removed from the Application	1. Examine application documentation to verify there is a documented process to remove code when it is no longer executed, and to ensure unnecessary code is not included into a release.	1. Procedures are documented for removing code when its no longer executed and ensuring unnecessary code is not included in a release. For a web-based application, the procedures include both .asp and .html files, to the extent they exist; for a database application, they include stored procedures; for a client server or distributed application they include the Visual Basic or C (or the programming language that is being used) modules.			
82	SI-2	DISA Application Security Checklist V2 R1.1 6050 5050		COTS/ Custom	The Application is Tested Prior to Update or Upgrade	1. Examine the application's configuration management plan (or similar document) to verify procedures exist which address the testing and implementation process for all patches, upgrades, and application deployments. 2. Examine test plans for the last several application releases.	1. Procedures are documented for the testing for all patches, upgrades and application deployments that is required as part of the agency's configuration management process. 2. A test plan and procedures are created and updated each production application release.			

Control ID	Out-of-Scope Reason
RA-1	Control covered in the MOT SCSEM
RA-2	Control covered in the MOT SCSEM
RA-3	Control covered in the MOT SCSEM
RA-4	Control covered in the MOT SCSEM
RA-5	Control covered in the MOT SCSEM
PL-1	Control covered in the MOT SCSEM
PL-2	Control covered in the MOT SCSEM
PL-3	Control covered in the MOT SCSEM
PL-4	Control covered in the MOT SCSEM
PL-5	Control not selected in IRS Publication 1075
PL-6	Control covered in the MOT SCSEM
SA-1	Control covered in the MOT SCSEM
SA-2	Control covered in the MOT SCSEM
SA-3	Control covered in the MOT SCSEM
SA-4	Control covered in the MOT SCSEM
SA-5	Control covered in the MOT SCSEM
SA-6	Control covered in the MOT SCSEM
SA-7	Control covered in the MOT SCSEM
SA-9	Control covered in the MOT SCSEM
CA-1	Control covered in the MOT SCSEM
CA-2	Control covered in the MOT SCSEM
CA-3	Control covered in the MOT SCSEM
CA-4	Control covered in the MOT SCSEM
CA-5	Control covered in the MOT SCSEM
CA-6	Control covered in the MOT SCSEM
CA-7	Control covered in the MOT SCSEM
PS-1	Control covered in the MOT SCSEM
PS-2	Control covered in the MOT SCSEM
PS-3	Control covered in the MOT SCSEM
PS-4	Control covered in the MOT SCSEM
PS-5	Control covered in the MOT SCSEM
PS-6	Control covered in the MOT SCSEM
PS-7	Control covered in the MOT SCSEM
PS-8	Control covered in the MOT SCSEM
CP-1	Control covered in the MOT SCSEM
CP-2	Control covered in the MOT SCSEM
CP-3	Control not selected in IRS Publication 1075
CP-4	Control covered in the MOT SCSEM
CP-6	Control covered in the MOT SCSEM

Control ID	Out-of-Scope Reason
CP-7	Control covered in the MOT SCSEM
CP-8	Control not selected in IRS Publication 1075
CP-9	Control not selected in IRS Publication 1075
CP-10	Control not selected in IRS Publication 1075
CM-1	Control covered in the MOT SCSEM
CM-8	Control covered in the MOT SCSEM
MA-1	Control covered in the MOT SCSEM
MA-2	Control covered in the MOT SCSEM
MA-3	Control covered in the MOT SCSEM
MA-4	Control covered in the MOT SCSEM
MA-5	Control covered in the MOT SCSEM
MA-6	Control not selected in IRS Publication 1075
MP-1	Control covered in the SDSEM
MP-2	Control covered in the SDSEM
MP-3	Control covered in the SDSEM
MP-4	Control covered in the SDSEM
MP-5	Control covered in the SDSEM
MP-6	Control covered in the SDSEM
PE-1	Control covered in the SDSEM
PE-2	Control covered in the SDSEM
PE-3	Control covered in the SDSEM
PE-4	Control covered in the SDSEM
PE-5	Control covered in the SDSEM
PE-6	Control covered in the SDSEM
PE-7	Control covered in the SDSEM
PE-8	Control covered in the SDSEM
PE-9	Control not selected in IRS Publication 1075
PE-10	Control not selected in IRS Publication 1075
PE-11	Control not selected in IRS Publication 1075
PE-12	Control not selected in IRS Publication 1075
PE-13	Control not selected in IRS Publication 1075
PE-14	Control not selected in IRS Publication 1075
PE-15	Control not selected in IRS Publication 1075
PE-16	Control covered in the SDSEM
PE-17	Control covered in the SDSEM
PE-18	Control covered in the SDSEM
PS-1	Control covered in the SDSEM
PS-2	Control covered in the SDSEM
PS-3	Control covered in the SDSEM

Control ID	Out-of-Scope Reason
PS-4	Control covered in the SDSEM
PS-5	Control covered in the SDSEM
PS-6	Control covered in the SDSEM
PS-7	Control covered in the SDSEM
PS-8	Control covered in the SDSEM
SI-1	Control covered in the MOT SCSEM
SI-3	Control covered in the MOT SCSEM
SI-4	Control covered in the MOT SCSEM
SI-5	Control covered in the MOT SCSEM
SI-8	Control not selected in IRS Publication 1075
IR-1	Control covered in the MOT SCSEM
IR-2	Control covered in the MOT SCSEM
IR-3	Control covered in the MOT SCSEM
IR-4	Control covered in the MOT SCSEM
IR-5	Control covered in the MOT SCSEM
IR-6	Control covered in the MOT SCSEM
IR-7	Control covered in the MOT SCSEM
AT-1	Control covered in the MOT SCSEM
AT-2	Control covered in the MOT SCSEM
AT-3	Control covered in the MOT SCSEM
AT-4	Control covered in the MOT SCSEM
IA-1	Control covered in the MOT SCSEM
IA-3	Control covered in operating system and network device SCSEMs
IA-4	Control covered in the MOT SCSEM
AC-1	Control covered in the MOT SCSEM
AC-4	Control covered in operating system and network device SCSEMs
AC-17	Control covered in the MOT SCSEM
AC-18	Control covered in the MOT SCSEM
AC-19	Control covered in the MOT SCSEM
AC-20	Control covered in the MOT SCSEM
AU-1	Control covered in the MOT SCSEM
AU-7	Control covered in the MOT SCSEM
AU-11	Control covered in the MOT SCSEM
SC-1	Control covered in the MOT SCSEM
SC-12	Control covered in the MOT SCSEM
SC-14	Control not selected in IRS Publication 1075
SC-15	Control covered in the MOT SCSEM
SC-17	Control covered in the MOT SCSEM
SC-18	Control covered in the MOT SCSEM

Control ID	Out-of-Scope Reason
SC-19	Control covered in the MOT SCSEM
SC-20	Control not selected in IRS Publication 1075
SC-22	Control not selected in IRS Publication 1075

References
Application Security and Development Checklist Version 2 Release 1.4, December 18, 2008
Federal Information Systems Control Audit Manual (FISCAM), GAO-09-232G February 2, 2009
NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, Revision 2

IRS Safeguard SCSEM Legend

Test Case Tab: Execute the test cases and document the results to complete the IRS Safeguard Computer Security review. Reviewer is required to complete the following columns: Actual Results, Comments/Supporting Evidence. Please find more details of each column below.

Test ID	Identification number of SCSEM test case
NIST ID	NIST 800-53/PUB 1075 Control Identifier
Source	Source of the test objective
Platform	Determines which platform the test case is applicable to, either a COTS application, or custom application.
Test Objective	Objective of test procedure.
Test Steps	Detailed test procedures to follow for test execution.
Expected Results	The expected outcome of the test step execution that would result in a Pass.
Actual Results	The actual outcome of the test step execution, i.e., the actual configuration setting observed.
Pass/Fail	Reviewer to indicate if the test case pass, failed or is not applicable.
Comments / Supporting Evidence	Reviewer to include any supporting evidence to confirm if the test case passed., failed on not applicable As evidence, provide the following information for the following assessment methods: 1. Interview - Name and title of the person providing information. Also provide the date when the information is provided. 2. Examination - Provide the name, title, and date of the document referenced as the evidence. Also provide section number where the pertinent information is resident within the document (if possible). 3. Test - Provide a detailed description of the output observed. Ensure all supporting evidence to verify the test case passed or failed. If the control is marked as NA, then provide appropriate justification as to why the control is considered NA.
Assumptions	

Change Log

Version	Release Date	Summary of Changes	Name
0.1	5/26/2009	First Release	Booz Allen